(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－325224
（P2001－325224A）
(43)公開日　平成13年11月22日(2001.11.22)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | ﾃｰﾏｺｰﾄﾞ(参考) |
|---|---|---|---|
| Ｇ０６Ｆ　15/00 | ３３０ | Ｇ０６Ｆ　15/00 | ３３０Ａ　５Ｂ０８５ |

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願2000－142970(P2000－142970)

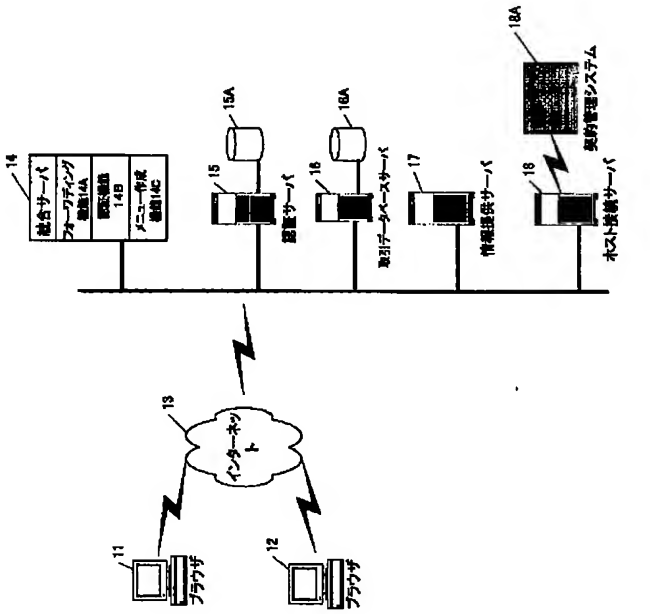
(22)出願日　平成12年５月16日(2000.5.16)

(71)出願人　399117110
日本ヒューレット・パッカード株式会社
東京都杉並区高井戸東３丁目29番21号
(72)発明者　小早川　直樹
東京都杉並区高井戸東３丁目29番21号　日本ヒューレット・パッカード株式会社内
(74)代理人　100081721
弁理士　岡田　次生　（外１名）

Ｆターム(参考)　5B085 AA08 AE00 AE23 CE03 CE04

(54)【発明の名称】　通信システム

(57)【要約】
【課題】ユーザが自己のアクセス権限の範囲を心配することなくメニューにしたがってウェブページをアクセスすることができるシステムを提供する。
【解決手段】この発明の通信システムは、複数のウェブサーバとブラウザとの間の通信を制御する統合サーバと、前記複数のウェブサーバが備えるファイルの少なくとも１つにアクセスする権限を有するユーザの識別情報およびアクセス権限情報を有する認証サーバと、を備え、統合サーバは、ユーザからのアクセス要求に応じて、認証サーバと通信しユーザのアクセス権限を確認し、アクセス権限に対応する項目を含んだメニューページを作成してユーザに返すダイナミック・メニュー作成機能を有する。一つの形態において、ダイナミック・メニューを作成するためのHTML文書であるテンプレートを備え、該テンプレートは、ユーザの属性に応じたページへのハイパーリンクの記述を含んでいる。



1

【特許請求の範囲】

【請求項１】複数のウェブサーバとブラウザとの間の通信を制御する統合サーバと、

前記複数のウェブサーバが備えるファイルの少なくとも１つにアクセスする権限を有するユーザの識別情報およびアクセス権限情報を有する認証サーバと、を備え、

前記統合サーバは、ユーザからのアクセス要求に応じて、前記認証サーバと通信し該ユーザの前記アクセス権限を確認し、該アクセス権限に対応する項目を含んだメニューページを作成してユーザに返すダイナミック・メニュー作成機能を有する通信システム。

【請求項２】前記ダイナミック・メニューを作成するためのHTML文書であるテンプレートを備え、該テンプレートは、ユーザの属性に応じたページへのハイパーリンクの記述を含んでいる請求項１に記載の通信システム。

【請求項３】ユーザの属性グループごとに用意された複数のページのＵＲＬを含む設定ファイルを備え、前記ハイパーリンクの記述は、前記属性グループに関する変数を含んでおり、前記ダイナミック・メニュー作成の際、アクセス中のユーザの前記属性グループに対応するＵＲＬが該変数に代入されるよう構成した請求項２に記載の通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ネットワーク・システムにおけるユーザ認証およびダイナミック・メニューの作成に関する。

【０００２】

【従来の技術】一般にネットワーク・システムにおいて、ユーザの認証はサーバ単位で実現している。業務上複数のサーバを設ける場合、ユーザ登録およびアクセス権限の設定はサーバごとに行なう。この方式では、ユーザの立場から、自己がどのサーバについてどういうアクセス権限を持っているかが判然とせず、実際にユーザＩＤおよびパスワードを入力してアクセスを試みて、アクセスを拒否されて自己にアクセス権限がないことを知ることがあった。さらに、それぞれのサーバ単位でユーザＩＤおよびパスワードの入力を要求され使い勝手が悪いという問題があった。

【０００３】特開平10-269184号公報には、証明証を利用して統合認証サーバがＤＢサーバおよび業務サーバに対するユーザのアクセス権限をチェックする方式が記載されている。

【０００４】また、特開平11-25048号公報には、統合認証サーバがクライエントから送られてくる統合証明書に関してアクセス権限をチェックし、正当であれば、通信当事者に証明書を送付し、通信を確立することが記載されている。

【０００５】

【発明が解決しようとする課題】これらの公開公報に記

2

載される技術は、複数のサーバに対するユーザの認証を統合するものではあっても、ユーザのアクセス権限の一覧をユーザに提示するものではないから、複雑にアクセス権限が設定されている場合、ユーザは自己にどの範囲のアクセス権限が設定されているかについて記憶しておくなり、アクセスの度にメモを参照する必要があるという問題を含んでいる。

【０００６】

【課題を解決するための手段】上記の課題を解決するため、この発明の通信システムは、複数のウェブサーバとブラウザとの間の通信を制御する統合サーバと、前記複数のウェブサーバが備えるファイルの少なくとも１つにアクセスする権限を有するユーザの識別情報およびアクセス権限情報を有する認証サーバと、を備え、統合サーバは、ユーザからのアクセス要求に応じて、認証サーバと通信しユーザのアクセス権限を確認し、アクセス権限に対応する項目を含んだメニューページを作成してユーザに返すダイナミック・メニュー作成機能を有する。

【０００７】このようにすることにより、ユーザには、ユーザのアクセス権限に応じたメニューページが提示されるので、ユーザは、自己のアクセス権限の範囲を心配することなく、メニューにしたがってウェブページをアクセスすることができる。

【０００８】この発明のシステムは、一つの形態において、ダイナミック・メニューを作成するためのHTML文書であるテンプレートを備え、該テンプレートは、ユーザの属性に応じたページへのハイパーリンクの記述を含んでいる。

【０００９】さらに具体的な形態において、この発明のシステムは、ユーザの属性グループごとに用意された複数のページのＵＲＬを含む設定ファイルを備え、ハイパーリンクの記述は、属性グループに関する変数を含んでおり、ダイナミック・メニュー作成の際、アクセス中のユーザの属性グループに対応するページのＵＲＬがこの変数に代入される。

【００１０】

【発明の実施の形態】次に図面を参照してこの発明の実施の形態を説明する。図１は、この発明の一実施形態のコンピュータ・ネットワークの全体的な構成を示すブロック図である。

【００１１】ブラウザ11、12は、典型的にはパーソナル・コンピュータに組み込まれた閲覧ソフトウェア、たとえばネットスケープ（商標）、インターネット・エクスプロアラ（商標）、によって実現され、インターネット13またはイントラネットを介してインターネット・プロトコルにより統合サーバ14に接続される。ブラウザと統合サーバ14との通信はＳＳＬ暗号機能を使用して行われる。

【００１２】統合サーバ14は、ブラウザから送信される認証CookieまたはユーザＩＤおよびパスワードを認証サ

ーバ15に送り、ユーザのアクセス権限の認証を行う認証機能14Bを備えている。

【００１３】ネットワークには複数のウェブサーバとして取引データベースサーバ16、情報提供サーバ17、およびホスト接続サーバ18が接続されている。たとえば保険業務での適用を例にとると、取引データベースサーバ16は代理店関連の取引データのデータベース16Aのためのウェブサーバである。情報提供サーバ17は、マニュアル、新商品などの情報を代理店および社員に提供するためのウェブサーバである。ホスト接続サーバ18は、契約管理システム18Aに接続するためのウェブサーバである。

【００１４】ダイナミック・メニューの構成

図２および図３を参照しながらダイナミック・メニューの構成を説明する。ダイナミックメニューは、たとえば図３に示す形態をとり、メニューページに埋め込まれてユーザのブラウザに表示される。この例ではNEW!新着情報のボタン42がダイナミックに作成されており、このボタンをクリックすると、アクセス中のユーザの属性グループに対応するページが表示される。ボタン43aから43eは、通常のハイパーリンクのボタンであり、ユーザの属性に関わらずそれぞれ同じウェブページにリンクされている。ボタン44は、パスワード変更手続きに入るためのもので、ボタン45は、ログアウトするためのボタンである。

【００１５】図２において、統合サーバ14のフォーワディング機能14Aは、インターネット13を介してブラウザ11、12と通信を行う機能である。ブラウザ11からのアクセスに対して認証サーバ15による認証がなされると、メニュー作成機能14CがHTML文書であるテンプレート32を読み出す。このテンプレートは、ボタン42を表示するために、たとえば改行タグ<BR>から始まる次に示す内容の記述を含んでいる。

【００１６】

```
<BR>
<TABLE CORDER=1 WIDTH=" 100%" >
<TR><TD ALIGN=" CENTER"  BGCOLOR=" #DDDD" >
<FONT COLOR=" #FF000" ><STRONG>NEW! </STRONG><FONT
>
<A HREF=" $S_NEW"  TARGET=" VIEW" >新着情報</A>
</TD></TR>
</TABLE>
```

【００１７】この記述の中で、<Aおよび</A>は、アンカータグと呼ばれ、ハイパーリンクを規定するタグである。この例では、「新着情報」と表示されるボタンをクリックすると、$S_NEWが示すＵＲＬにページが飛ぶことを規定している。$S_NEWは、ユーザの属性に応じて設定ファイル31から読み出されて代入されるＵＲＬである。したがって、ユーザに送信されるメニューページにおいては、$S_NEWの箇所に具体的なＵＲＬが入れられている。

【００１８】設定ファイル31は、たとえば次の表に示す内容を含んでいる。この例ではユーザの属性としてユーザの所属するグループをとっている。

【００１９】

【表１】

| 所属グループ | 表示するページのＵＲＬ |
|---|---|
| grp00 | https://www.abc.co.jp/xyz/whatsnew1 |
| grp01 | https://www.abc.co.jp/xyz/whatsnew2 |
| grp02 | https://www.abc.co.jp/xyz/whatsnew3 |
| grp03 | https://www.abc.co.jp/xyz/whatsnew4 |
| grp04 | https://www/abc.co.jp/xyz/whatsnew5 |

【００２０】ユーザからのアクセス要求があると、後にアクセス制御のセクションで説明するように、認証サーバ15のアクセス権限チェック機能15BがユーザＩＤまたはユーザの属性を記述する情報に基づいてユーザの所属グループを判断する。いまの場合、ユーザがgrp02に所属するとすると、統合サーバは、https://www.abc.co.jp/xyz/whatsnew3を表１の設定ファイルから読み出し、テンプレート32における上述のアンカー中の$S_NEWに代入する。こうして作成されたメニューページがブラウザ11に送られる。

【００２１】こうしてブラウザ11に表示されたメニューページでは、新着情報のボタン42は、https://www.abc.co.jp/xyz/whatsnew3にハイパーリンクが形成されている。したがって、このボタンをクリックすると、whatsnew3のページがブラウザに表示される。こうしてユーザには、ユーザに適した項目だけのページが提示される。

【００２２】ユーザ認証

次に図４を参照してユーザ認証のプロセスを説明する。ブラウザ11がhttpプロトコルにしたがって統合サーバ14にアクセス要求を送ると（101）、統合サーバ14、より具体的には図１におけるフォーワディング機能14A、がこれを受信し、認証Cookieの有無をチェックする（102）。Cookie（クッキー）は、httpプロトコルで使われる小さいファイルであり、サーバ側のスクリプトから任意の情報を詰めてブラウザに送られる。この実施例における認証Cookieは、後に説明するように認証が成功したときブロック123で設定されてブラウザ11に送られるものである。

【００２３】認証Cookieがないときは、統合サーバ14はログインページのhtmlファイルを読み出してブラウザに送る（104）。ユーザがブラウザ11に表示されるログインページにユーザＩＤおよびパスワードを入力して送信すると、統合サーバ14は、送られてきた情報を用いてユーザ認証メッセージを作成し、認証サーバ15に送る（106）。これに応答して認証サーバ15は、記憶装置15Aに格納されているユーザＩＤおよびユーザパスワードと送信されてきたユーザＩＤおよびユーザパスワードとの整合性をチェックし（107）、整合しなければ、ＮＧ応答メッセージを統合サーバに返す（108）。これを受けて統合サーバ14は、ログインエラーページを生成してブラウザ11に送る。ＮＧの原因がパスワードの期限切れの場合は、統合サーバ14は、パスワード変更ページをブラウザ11に送る（109）。

【００２４】ログインエラーページまたはパスワード変更ページは、ブラウザ11に表示され（110）、ユーザは再度ログインを試み、またはパスワードの変更手続きをすることができる。

【００２５】ブロック107にもどり、ユーザ認証がＯＫの場合、認証サーバ15は、認証がＯＫであることを示すデータを入れた認証Cookieを作り（121）、ＯＫメッセージとともに統合サーバ14に送る（122）。統合サーバ14は、認証Cookieを設定し、図５のアクセス制御プロセスに移るとともに、ブラウザ11に認証Cookieを送る（123）。ブラウザ11は、認証Cookieをそのユーザ固有の情報として保存し、次に統合サーバ14にアクセスするときに統合サーバ14に送信する。ブロック102にもどると、統合サーバ14は、ブラウザからのアクセス要求に認証Cookieがついていると、図５のアクセス制御プロセスに移る。

【００２６】認証サーバは、統合サーバ14に接続したユーザのユーザＩＤを保持し、接続から切断までのサービス選択状況を監視し、その記録（ログ）をとる。また、認証サーバ15は、無停止を前提として構成されており、システムの稼働中に新規ユーザの登録や既存のユーザの削除を実行することができる。

【００２７】アクセス制御

統合サーバ14は、アクセス要求メッセージを認証サーバ15に送る（204）。これを受けて認証サーバ15は、認証Cookieのチェックを行い、有効であればこのユーザが要求中のファイルへのアクセス権限をもつかどうかをアクセス権限テーブルを参照してチェックする（206）。このユーザがアクセス権限を持っていることが確認されると、認証サーバ15は、ＯＫメッセージを統合サーバ14に送る（207）。アクセス権限テーブルは、たとえば次のようなconfig情報として記述されている。

【００２８】

【表２】Config1　（URL情報）

URL01, grp01
URL02, grp02
URL03, grp01, grp02
URL04, grp02, grp03

Cinfig2　（ユーザおよびグループ情報）

grp01, UID=A1*
grp01, UID=A2001
grp01, UID=A3009
grp02, DESCRIPTION=*0101
grp03, DESCRIPTION=*1010

【００２９】ここで、”*”は、ワイルドカードで任意の数の任意の文字がこの位置にあってもよいことを意味する。UIDは、ユーザＩＤであり、DESCRIPTIONは、ユーザＩＤ以外のユーザの属性を表すコードであり、企業内の管理職コード、専門職コード、部門コードなどがその例である。表２のConfig表現をテーブル表示すると次の表３のようになる。

【００３０】

【表３】

| 文書 | grp01 | | | grp02 | | grp03 |
|---|---|---|---|---|---|---|
| | A1* | A2001 | A3009 | B0101 | C0101 | C1010 |
| URL01 | ○ | ○ | ○ | | | |
| URL02 | | | | ○ | ○ | |
| URL03 | ○ | ○ | ○ | ○ | ○ | |
| URL04 | | | | ○ | ○ | ○ |

【００３１】表３では、DESCRIPTION=*0101に該当する属性コードとして、B0101およびC0101があり、DESCRIPTION=*1010に該当する属性コードとしてC1010があるものと仮定している。このようにアクセス権限は、ＵＲＬ文書単位、グループ単位で設定することができる。

【００３２】統合サーバ14は、認証サーバ15からＯＫメッセージを受け取ると、httpリクエストヘッダを作成してウェブサーバ、今の例では情報提供サーバ17に送られる（220）。こうして要求されたコンテンツがブラウザ11に表示される（224）。

【００３３】ブロック205で認証Cookieが不正であったり、期限切れであると、認証サーバ15は、ＮＧメッセージを統合サーバ14に送り（208）、統合サーバ14は、ＮＧの理由に応じて再ログインページまたはエラーページをブラウザ11に送る（209）。こうしてブラウザ11に再ログインページまたはエラーページが表示され（21

0）、ユーザはログインを再試行し、またはエラーを訂正することができる。

【００３４】統合サーバから認証サーバへのアクセス権限確認処理は、標準的なＬＤＡＰプロトコルを用いるが、その他のプロトコルを用いることができることはもちろんである。

【００３５】ダイナミックメニュー生成プロセス

次に図６を参照してダイナミックメニュー（動的メニュー）の生成プロセスを説明する。ユーザがブラウザ11から統合サーバ14にダイナミックメニューを要求すると（301）、統合サーバ14は、要求に認証Cookieが付いているかどうかをチェックし（302）、付いていなければログインエラーページをブラウザ11に返（303）、ログインから認証シーケンス（図２）に移る。ダイナミックメニューの要求に認証Cookieが付いていると、統合サーバ14は、メニュー要求メッセージを認証サーバ15に送る（304）。これを受けて認証サーバ15は、アクセス権限をチェックし（305）、このユーザのアクセス権限を示す応答メッセージを統合サーバ14に返す（305）。

【００３６】これに応答して統合サーバ14は、メニューテンプレート32を読み込み、認証サーバ15からの応答メッセージで特定されたこのユーザの所属グループに対応するＵＲＬを設定ファイル31から読み出してメニューテンプレート３２に埋め込む（309）。こうして生成されたダイナミックメニューページがブラウザ11に送られ、ブラウザ11にダイナミックメニューが表示される。このダイナミックメニューのメニュー項目にはハイパーリンクが生成されており、ユーザがメニュー項目をクリックすると該当するページへのアクセス要求がブラウザ11から統合サーバ14に送られ、図５に関連して説明したアクセス制御のシーケンスに入る。

【００３７】以上にこの発明を具体的な実施の形態を例にとって説明したが、この発明は、このような実施の形態に限定されるものではない。

【図面の簡単な説明】

【図１】この発明の一実施例のネットワークシステムの全体的な構成を示すブロック図。

【図２】ダイナミックメニューの生成を行うためのシステムの構成を示すブロック図。

【図３】ブラウザに表示されるダイナミックメニューの例を示す図。ローチャート。

【図４】ユーザ認証プロセスを示すフローチャート。

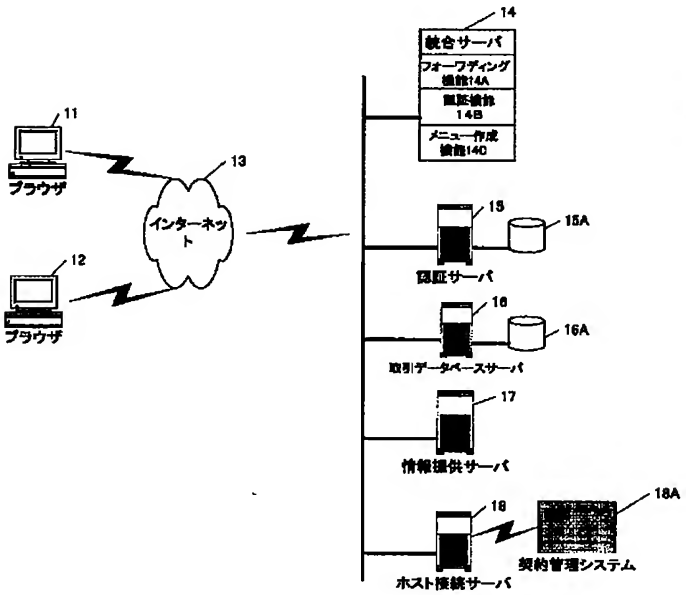
【図５】アクセス制御のプロセスを示すフローチャート。

【図６】ダイナミックメニューの生成プロセルを示すフローチャート。

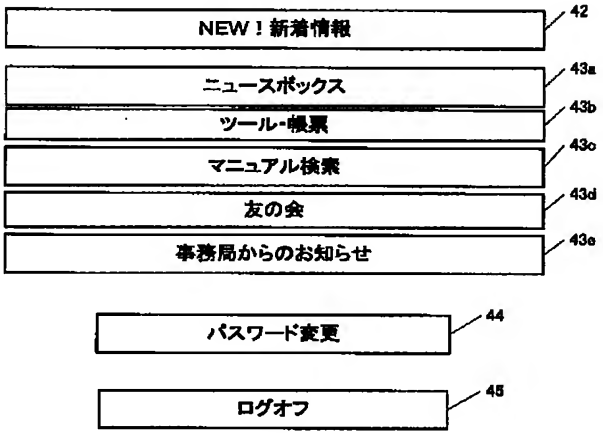
【符号の説明】

１１、１２　　ブラウザ
１４　　統合サーバ
１５　　認証サーバ
１６、１７、１８　　ウェブサーバ

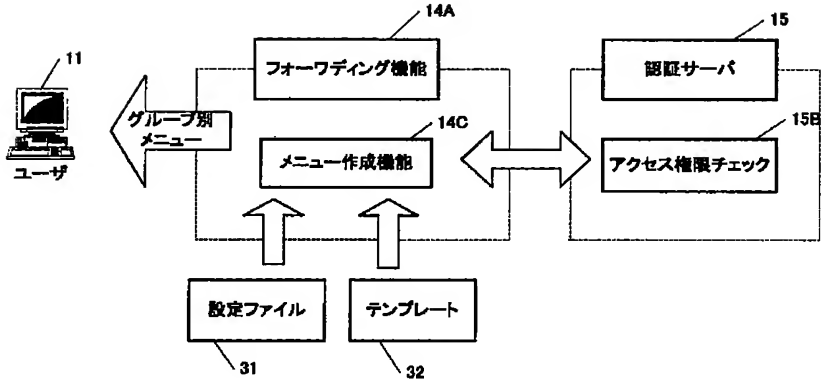
【図１】



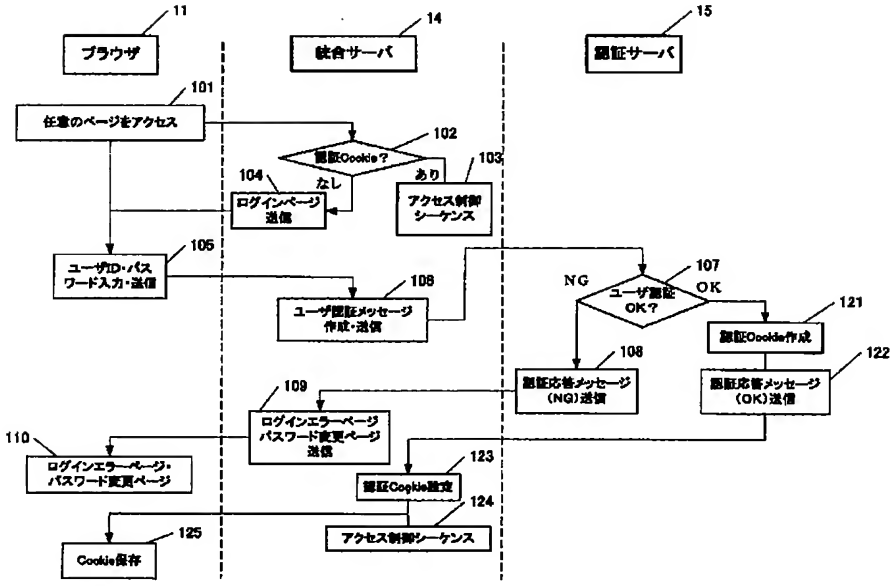

【図３】



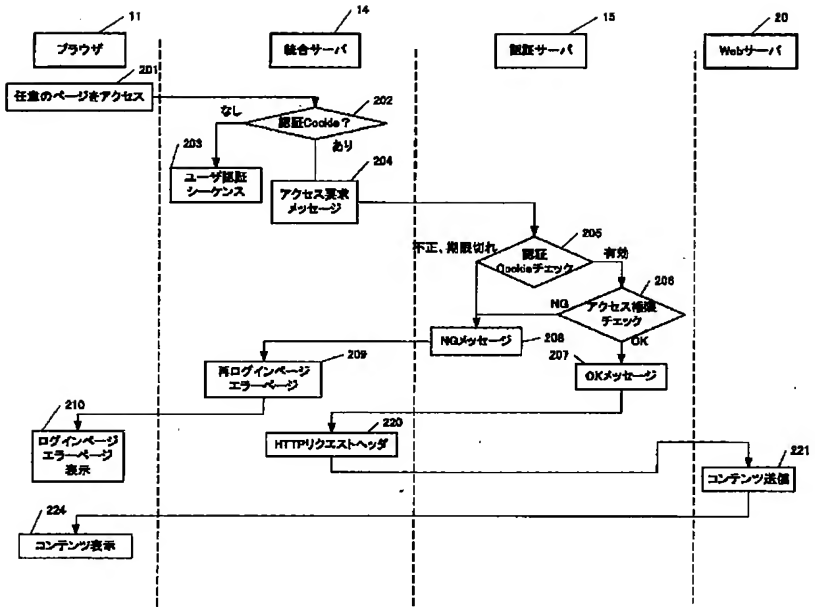
【図２】


14A
15
11
フォーワディング機能
認証サーバ
グループ別
メニュー
14C
15B
メニュー作成機能
アクセス権限チェック
ユーザ
設定ファイル
テンプレート
31
32

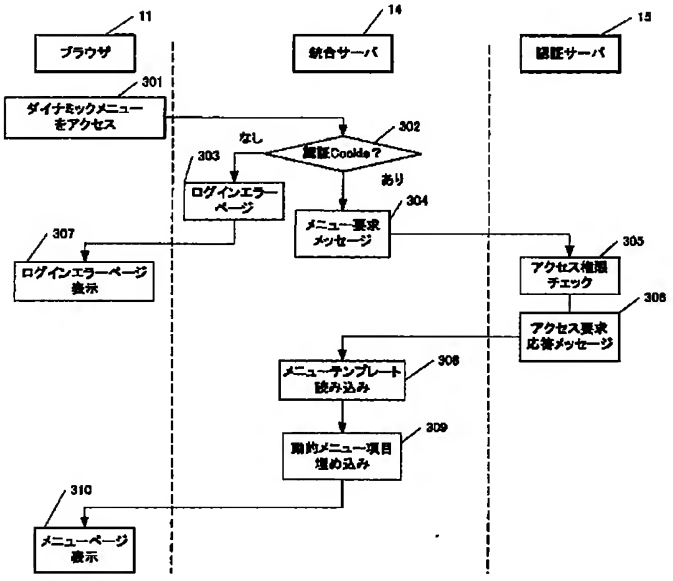
【図４】


11
14
15
ブラウザ
統合サーバ
認証サーバ
101
任意のページをアクセス
102
認証Cookie?
あり
103
なし
104
ログインページ
送信
アクセス制御
シーケンス
105
ユーザID・パス
ワード入力・送信
108
ユーザ認証メッセージ
作成・送信
107
NG
ユーザ認証
OK?
OK
121
認証Cookie作成
108
認証応答メッセージ
(NG)送信
122
認証応答メッセージ
(OK)送信
109
ログインエラーページ
パスワード変更ページ
送信
110
ログインエラーページ・
パスワード変更ページ
123
認証Cookie設定
124
アクセス制御シーケンス
125
Cookie保存

【図５】


11
ブラウザ
14
統合サーバ
15
認証サーバ
20
Webサーバ
201
任意のページをアクセス
202
認証Cookie？
なし
あり
203
ユーザ認証シーケンス
204
アクセス要求メッセージ
205
認証Cookieチェック
不正、期限切れ
有効
206
アクセス権限チェック
NG
OK
NGメッセージ
208
207
OKメッセージ
209
再ログインページエラーページ
210
ログインページエラーページ表示
220
HTTPリクエストヘッダ
221
コンテンツ送信
224
コンテンツ表示

【図６】


11
ブラウザ
14
統合サーバ
15
認証サーバ
301
ダイナミックメニューをアクセス
302
認証Cookie？
なし
あり
303
ログインエラーページ
304
メニュー要求メッセージ
307
ログインエラーページ表示
305
アクセス権限チェック
306
アクセス要求応答メッセージ
308
メニューテンプレート読み込み
309
期約メニュー項目埋め込み
310
メニューページ表示